



桃園區網中心 第 63 次管審會議

國立中央大學 電算中心

報告人：陳奕翰

2019 / 01 / 10



桃園區網中心

概況報告

漏洞預警-CSRF

網路印表機存在漏洞

2019年

資安三大重點警示

資安宣導事項



漏洞預警 - CSRF

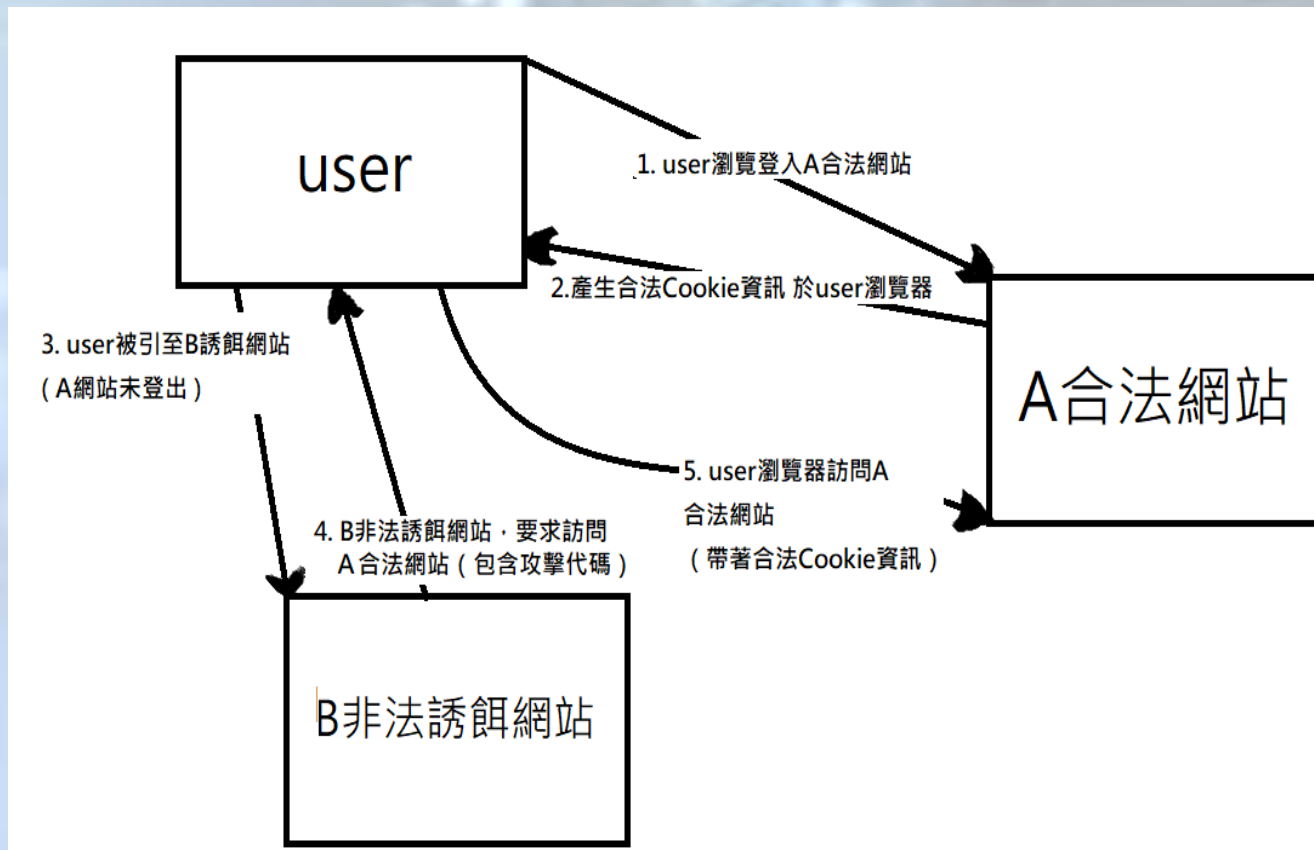
電子學習平台Moodle出現嚴重CSRF缺陷：

- 開源電子學習平臺Moodle出現跨站請求偽造漏洞

能讓使用者身分驗證後與Moodle連線的期間，被有心人士冒名操作。

這項弱點來自Moodle登入表單的安全機制，伺服器端透過 `authenticate_user_login()` 函數，驗證使用者的請求是否合法，同時也可以一併檢查位於 `..\core\session\manager` 路徑之Token，不過，這項功能預設並未啟動。而外掛驗證工具或是內建的密碼變更模組執行時，上述的函數驗證請求的效力仍在，但缺乏Token檢驗，因此若是攻擊者加入新的組態參數 `$CFG->>disablelogintoken`，就能製造跨站請求偽造攻擊，迴避Moodle對所有表單內的Token內容偵測。

CSRF 攻擊行為：



[影響平台:]

Moodle 3.5.2、3.4.5、3.3.8、3.1.14以前版本

[建議措施:]

下載Moodle 3.6、3.5.3、3.4.6、3.3.9、3.1.15等修補版

[參考資料:]

1. <https://moodle.org/mod/forum/discuss.php?d=378731>
2. <http://git.moodle.org/gw?p=moodle.git>
3. <https://www.auscert.org.au/bulletins/72006>
4. <https://securitytracker.com/id/1042154>
5. <https://zh.wikipedia.org/wiki/%25E8%25B7%25A8%25E7%25AB%2599%25E8%25AF%25B7%25E6%25B1%2582%25E4%25BC%25AA%25E9%2580%25A0>
6. <https://zh.wikipedia.org/wiki/Moodle>
7. <https://itw01.com/FRIYWES.html>
8. <http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-63183>
9. <http://git.moodle.org/gw?p=moodle.git>
10. <http://git.moodle.org/gw?p=moodle.git>
11. <http://www.firnbergschulen.at/wp-content/uploads/2016/09/moodle-banner.png>
12. <https://www.ithome.com.tw/news/127237?fbclid=IwAR3IAHltI7sITzvckc49GOh6qqZqLWO-5VsgL3XybeVqwoHaEs6cnAm0GK0>



漏洞預警 - 網路印表機存在漏洞

網路印表機設備未正確設置存在漏洞

- TWCERT/CC於2018/12/20接獲外部通報，經過shodan搜尋過後共有大約1400台網路印表機設備暴露在公開網路中。
- 其中大多數控制頁面並未使用身份驗證，有些是Daemon暴露在公開網域上 (e.g. LPD on port 515)，總覽：(query: JetDirect country:tw)，發現單位網路印表機設備未正確設置存在漏洞，攻擊者可利用此漏洞進行惡意攻擊

- [影響平台:]
網路印表機設備 HP JetDirect系列
- [建議措施:]
 - 1.清查內部是否有使用相關網路印表機設備，建議更新至最新修補程式，亦建議更換系統使用者之相關密碼。若暫時無異常行為，建議持續觀察一個星期左右。
 - 2.可能的話將印表機轉為內部網路架構使用，並限制外部存取來源
 - 3.安裝防毒軟體並更新至最新版，並注意病毒碼須持續更新。



2019年資安三大重點警示 (一)

憑證資料外洩遭盜用詐騙事件：

- 網裝置普及之下，民眾往往會設定相同的帳號密碼，但若是某家企業發生個資外洩事件時，駭客就會利用殭屍網路（Botnet）大軍，使用大量外流的帳號密碼，自動化地登入其它網站，就會造成資料外洩的連鎖效應。
- 對消費者所造成的直接影響，可能出現在信用卡哩程累積回饋遭盜用、個人社群帳號被入侵，藉此散播惡意評論等，至於在企業端方面，除了業務營運受到波及與商譽受損，甚至可能因未善盡資料保護義務，觸犯法規而遭受罰鍰處分。

防護措施：

盡量不要重複使用相同的帳號密碼，通過雙重認證的方式防護。

企業做好機密防護措施，杜絕大量個資外流的事件發生。

(引用資料 - 趨勢科技)

<https://goo.gl/IPxiFe>





2019年資安三大重點警示 (二)

網路釣魚攻擊手段將成為主要攻擊手法：

網路釣魚將會明顯增加：

- 現在多元裝置，以及操作系統趨勢下，駭客將不再透過單一軟體系統層面的漏洞攻擊，反而利用簡訊、通訊軟體進行網路釣魚攻擊
- 1. **不要隨意點擊不明連結：**
- 駭客特別會利用時事議題、網路紅人的傳散能力，進行水坑式攻擊，植入惡意程式的連結或是訊息 騙取追蹤粉絲點閱，使得粉絲遭牽連受駭，造成個人資料與財物損失。
- 2. **SIM卡劫持手法 (SIM-jacking)**
- 犯罪者取得個人電話號碼和資訊，假冒手機用戶，向電信廠商技術服務人員申辦新的**SIM**卡，之後透過簡訊存取用戶的帳號資料，甚至盜用電子錢包。

(引用資料 - 趨勢科技)

<https://goo.gl/1PxiFe>



2019年資安三大重點警示 (三)

工控系統的安全性：

- 1.智慧自動化的普及，所延伸的資安趨勢，企業營運比以往更加仰賴即時數據，因此ICS網路必須能與企業網路連結。
- 2.駭客將不安全的企業網路設備當成跳板，再移轉到最容易攻擊的ICS設備和資料庫。
- 透過AI預測判定企業管理階層和特定對象的相關動向，進而取信周圍相關人士進行入侵威脅。

1.應培養資安意識，對於電子郵件或是通訊軟體上的訊息提高警覺，降低遭受網路釣魚詐騙的風險。

2.安裝防毒軟體，協助保護個人資料、交易安全。

3.定期更新密碼，使用多重認證的帳密保護措施，或是密碼管理工具以保護相關憑證資訊，也可幫助個人機密資料的保護。

(引用資料 - 趨勢科技)

<https://goo.gl/IPxiFe>



資安宣導事項

2018申請檢測統計

原申請時間為每年8月，2019年起增加上半年2月申請時段。

申請學校	弱點掃描(GFI LANguard)	網頁檢測(IBM APP scan)	追蹤處理情形
大興高中	1	1	已追蹤10/31
南亞技術學院	10	2	已追蹤10/31
至善高中	2	0	已追蹤10/31
萬能科技大學	0	2	已追蹤10/31
啟英高中	4	1	已追蹤10/31
中原大學	23	11	已追蹤10/31
元智大學	0	5	已追蹤10/31
永平工商	2	3	已追蹤10/31
總量	42	25	已追蹤10/31



LANguard

需協助弱點掃描，請將此 IP 設為白名單

140.115.2.130

The screenshot displays the GFI LanGuard web interface. The top navigation bar includes links for 儀表板 (Dashboard), 掃描 (Scan), 補救 (Remediation), 活動監視器 (Activity Monitor), 報告 (Reports), 組態 (Configuration), and 公用程式 (Utilities). The main content area features a welcome message, a network vulnerability level gauge, and a large blue banner for GFI LanGuard. The gauge shows a score of 1, indicating a low level of vulnerability. The banner text reads "GFI LanGuard™ Network Scanning and Patch Management". Below the banner, there is a section for "最新資訊" (Latest News) with two entries dated 13-八月-2018, both mentioning updates for Google Chrome and UltraVNC. A yellow warning bar at the bottom states: "您有一部傳送/伺服器管理超過 100 部電腦" (You have one server managing more than 100 computers).

電腦
TrendMicro
AntiThrea...

資源回收筒
supportusto...

Mozilla Firefox

SEP12_1_6

GFI LanGuard

GFI LanGuard
Central Man...

GFI LanGuard

儀表板 掃描 補救 活動監視器 報告 組態 公用程式

歡迎使用 GFI LanGuard
GFI LanGuard 正準備稽核您的網路弱點。

網路弱點層級
LanGuard 已自動啟動本機電腦上的弱點稽核。

檢視儀表板
調查網路弱點狀態並稽核結果。

GFI LanGuard™
Network Scanning and Patch Management

GFI

最新資訊

13-八月-2018 - 修補程式管理 - 新增對 Google Chrome 68.0.3440.106 的支援 - [讀取更多](#)

13-八月-2018 - 修補程式管理 - 新增對 UltraVNC 1.2.1.0 的支援 - [讀取更多](#)

您有一部傳送/伺服器管理超過 100 部電腦



IBM APP scan

桃園區網中心掃前，與老師們討論掃描時間
並請貴單位將此**IP**開設白名單
報告整理好壓縮後加密寄回。

檢測網頁分析的網址	檢測網頁分析的網址	檢測網頁分析的網址	檢測網頁分析的網址
www.ypvs.tyc.edu.tw	webmail.ypvs.tyc.edu.tw	ep.ypvs.tyc.edu.tw	
http://www.dxhs.tyc.edu.tw/ischool/publi			
web.cyvs.tyc.edu.tw			
www.nanya.edu.tw	www.lib.nanya.edu.tw		
www.vnu.edu.tw			
www.vnu.edu.tw	saip.vnu.edu.tw/admisstion		
https://140.138.78.94	http://www.infocom.yzu.edu.tw/index.php/	http://www.cm.yzu.edu.tw/CH/Index.aspx	http://www.ee.yzu.edu.tw/



宣導事項

桃園區網聯絡人：陳奕翰

Email : tanet_ncu@cc.ncu.edu.tw

電話：03 -4227151#57514

網管通訊錄更新

- 若單位名稱、網管人員及聯絡方式有變動，請與區網聯絡更新。

教育訓練 | 講座 | 會議

- 原則上都安排在星期四

校園資安推廣

- 推廣對象：教職員及學生均可
- 徵求連線單位講師支援(具有資安相關證照或相關研究)